Lazarus Alliance
Proactive Cyber Security©

2026 CMMC Assessment Benchmark Report

Aggregate Anonymized Insights from Lazarus Alliance
CMMC Level 2 C3PAO Assessments

Reporting Period: January 2025 – June 2026 • Published August 2026

17 days	68	74%	89%
Median Assessment Duration	Avg. In-Scope Systems	Assessments with ≥1 POA&M;	Required Additional Evidence

Lazarus Alliance, Inc.
Authorized CMMC C3PAO (CPN 10251)
A2LA-Accredited FedRAMP 3PAO • PCI DSS QSA • Veteran-Owned Small Business

1. Purpose & Methodology

This benchmark report aggregates anonymized findings from formal CMMC Level 2 certification assessments performed by Lazarus Alliance as an authorized Cyber AB C3PAO (CPN 10251) between January 2025 and June 2026. All organizational identifiers, system names, contract numbers, and proprietary details have been removed. Figures represent observed patterns across the assessment population and are intended to provide defense industrial base (DIB) organizations with realistic expectations for scope, duration, evidence quality, and common control gaps.

Scope of Data: Completed Level 2 assessments only (self-assessment / SPRS data and readiness engagements are excluded). Both enclave and enterprise boundary assessments are included. Numbers are rounded for clarity and confidentiality.

Disclaimer: *These benchmarks are observational and do not constitute guarantees of future performance, certification outcomes, or timelines. Individual results vary significantly based on preparation quality, environment complexity, inheritance, and assessor findings. Lazarus Alliance maintains strict independence and impartiality under ISO/IEC 17020 and Cyber AB requirements.*

2. Executive Summary – Key Benchmarks

Across the aggregated assessment population, organizations that entered formal assessment with mature documentation, complete logging, and verified multifactor authentication experienced materially shorter cycles and fewer residual findings. The data below reflect the full observed distribution.

Metric	Observed Value	Notes
Average scope size (in-scope systems / assets)	~68 systems / ~155 endpoints	Wide range: 12–410 systems
Median formal assessment duration	17 business days	Kickoff to draft SAR; excludes readiness
Assessments resulting in ≥1 POA&M; item	74%	Most POA&Ms; closed within 180-day window
Percentage requiring additional evidence	89%	Typically during evidence review phase
Enclave vs. Enterprise boundary	67% Enclave / 33% Enterprise	Enclaves dominate smaller DIB contractors
Average evidence volume submitted	~1,920 discrete artifacts	Range approximately 650–5,800

3. Average Scope Size

Scope size remains the primary driver of assessment effort and cost. Across the dataset:

- Average in-scope systems/assets: **approximately 68**
- Average endpoints (workstations, servers, network devices): **~155**
- Median user population within the assessment boundary: **~95 users**
- Smallest observed scope: 12 systems (tightly defined CUI enclave)
- Largest observed scope: 410+ systems (full enterprise boundary with multiple locations)

Organizations that successfully limited scope through well-documented enclaves, network segmentation, and clear CUI data-flow diagrams consistently experienced shorter assessment windows and fewer findings related to residual enterprise systems.

4. Median Assessment Duration

Formal assessment duration is measured from assessment kickoff (evidence package acceptance) through delivery of the draft Security Assessment Report (SAR). Readiness / gap-analysis periods are excluded.

- **Median formal assessment duration: 17 business days**
- 25th percentile: 11 business days (highly prepared, smaller enclave scopes)
- 75th percentile: 26 business days
- Outliers exceeding 35 business days typically involved multi-site enterprise boundaries or significant evidence remediation mid-assessment

Organizations that leveraged automated evidence collection (including Continuum GRC / IT Audit Machine® workflows) and completed pre-assessment evidence mapping generally fell into the lower quartile of duration.

5. Common Failed Objectives

The following practices most frequently generated findings (partial implementation or not met) across Level 2 assessments. Rankings reflect frequency of residual findings after initial evidence review:

Rank	Practice	Domain	Primary Issue Observed
1	IA.L2-3.5.3	Identification & Authentication	Multifactor authentication incomplete for privileged or remote access paths
2	AU.L2-3.3.1 / 3.3.2	Audit & Accountability	Incomplete or non-centralized audit logging; retention or review deficiencies
3	CM.L2-3.4.1 / 3.4.2	Configuration Management	Missing or outdated baselines; configuration change control gaps
4	AC.L2-3.1.1 / 3.1.2	Access Control	Account management / least privilege not fully enforced or evidenced
5	SI.L2-3.14.1 / 3.14.2	System & Information Integrity	Flaw remediation / vulnerability scanning cadence or coverage incomplete
6	SC.L2-3.13.1 / 3.13.5	System & Communications Protection	Boundary protection / external system connections insufficiently controlled
7	MP.L2-3.8.1 / 3.8.3	Media Protection	Media sanitization / CUI media handling procedures lacking evidence

Practices related to continuous monitoring, incident response testing, and personnel security screening also appeared frequently among residual findings, particularly in organizations with limited dedicated security staff.

6. Evidence Deficiencies

Evidence quality—not merely volume—determined assessment efficiency. The most common deficiencies observed:

- **Screenshots without context or timestamps** – images lacking system identifiers, dates, or configuration paths
- **Policy statements without operational evidence** – documented procedures that could not be demonstrated in practice
- **Incomplete log samples** – audit records missing required event types or covering insufficient time periods
- **Missing configuration baselines** – no authoritative, version-controlled baseline for comparison
- **Inheritance claims without supporting SSP or customer responsibility matrix**
- **Outdated or generic templates** – policies not tailored to the actual environment or CUI flows
- **Lack of sampling methodology documentation** for larger environments

Assessors consistently noted that organizations using structured evidence repositories (tagged by practice, with clear ownership and last-reviewed dates) required far fewer clarification requests.

7. POA&M; Frequency

Plans of Action and Milestones remain a normal and expected outcome for many first-time Level 2 assessments.

- **74% of assessments** resulted in at least one POA&M; item
- Median number of POA&M; items per assessment with findings: **3**
- Most common POA&M; categories: multifactor authentication gaps, logging completeness, vulnerability management cadence, and media protection procedures
- Organizations that closed POA&Ms; within the allowed window and provided clear evidence of remediation achieved Final Level 2 status without further delay in the large majority of cases

Importantly, the presence of a limited, well-scoped POA&M; did not prevent successful certification when residual risk was properly documented and remediated on schedule.

8. Enclave vs. Enterprise Environments

Boundary definition continues to be one of the highest-leverage decisions an Organization Seeking Certification (OSC) can make.

- **67% of assessments** used a defined CUI enclave (segmented boundary)
- **33%** assessed a full enterprise or multi-site boundary
- Enclave assessments showed lower average duration, lower evidence volume, and fewer residual findings related to residual enterprise systems
- Enterprise assessments more frequently encountered issues with consistent policy application, remote access, and multi-location logging

Successful enclave strategies depended on accurate data-flow diagrams, enforced network segmentation, and clear documentation of what is inside versus outside the assessment boundary. Assessors required strong evidence that CUI could not traverse uncontrolled paths.

9. Average Evidence Volume & Additional Evidence Requests

Evidence volume alone is a weak predictor of success; relevance and completeness matter more.

- Average discrete artifacts submitted: **~1,920** (policies, procedures, screenshots, logs, diagrams, configurations, tickets, training records, etc.)
- Observed range: approximately 650 to 5,800 artifacts
- **89% of assessments** required at least one round of additional evidence after initial package review
- Most frequent additional requests: expanded log samples, configuration baseline details, MFA coverage proof for specific access paths, and media sanitization records

Organizations that pre-mapped every practice to specific evidence artifacts and performed internal mock assessments experienced the lowest rates of mid-assessment evidence requests.

10. Most Misunderstood Requirements

Certain practices generated repeated clarification questions or incorrect interpretations even among otherwise well-prepared organizations:

- **IA.L2-3.5.3 (Multifactor Authentication)** – Scope of “privileged accounts” and remote access paths frequently under-interpreted; application-layer MFA sometimes omitted.
- **AU.L2-3.3.1 / 3.3.2 (Audit Events & Content)** – Confusion between “what must be logged” versus “what is retained and reviewed.” Review cadence and protected storage of logs often incomplete.

- **CM.L2-3.4.1 (Baseline Configurations)** – Belief that a generic hardening checklist equals a maintained, version-controlled baseline for the actual in-scope systems.
- **AC.L2-3.1.12 / 3.1.20 (Remote Access & External Connections)** – Underestimation of the need to control and monitor all external system connections that can access CUI.
- **SC.L2-3.13.11 (FIPS-validated cryptography)** – Misapplication of FIPS requirements to non-CUI data paths or incomplete module validation evidence.
- **CA.L2-3.12.2 (Plan of Action)** and continuous monitoring expectations – Treating assessment as a point-in-time event rather than demonstrating ongoing control effectiveness.
- **Inheritance and Shared Responsibility** – Incomplete or unsupported claims of control inheritance from cloud or managed service providers without corresponding customer responsibility matrices or SSP excerpts.

Clear, environment-specific implementation statements mapped to actual technical and procedural evidence remain the most effective way to avoid these misunderstandings.

11. Key Insights for Organizations Seeking Certification

Patterns across the dataset point to several high-impact preparation practices:

1. **Define and defend the boundary early.** Well-documented enclaves with clear data-flow diagrams reduced both duration and findings.
2. **Treat evidence as a living system.** Timestamped, practice-mapped, and context-rich artifacts dramatically lowered clarification cycles.
3. **Prioritize MFA, logging, and baselines.** These three areas accounted for a disproportionate share of residual findings.
4. **Perform a realistic internal mock assessment.** Organizations that stress-tested their evidence package before engaging the C3PAO required fewer additional evidence requests.
5. **Accept that limited POA&Ms; are common.** Focus on rapid, well-documented remediation rather than attempting zero findings at all costs.
6. **Leverage automation where appropriate.** Structured GRC platforms that maintain continuous evidence and control status reduced both preparation time and assessment friction. Ensure that SaaS solutions are FedRAMP Moderate certified such as Continuum GRC ITAM.

12. About This Report & Contact

Lazarus Alliance is an authorized CMMC Third-Party Assessment Organization (C3PAO, CPN 10251), an A2LA-accredited FedRAMP 3PAO, a PCI DSS Qualified Security Assessor (QSA), and a veteran-owned small business headquartered in Scottsdale, Arizona. Since 2000 the firm has specialized in proactive cybersecurity, audit, and compliance services across CMMC, FedRAMP, SOC 2, NIST, ISO, and related frameworks.

This report is published for educational and benchmarking purposes. It does not constitute legal, contractual, or certification advice. Organizations preparing for CMMC Level 2 assessment are encouraged to engage qualified readiness support and to verify current Cyber AB and DoD requirements independently.

Lazarus Alliance, Inc.
27743 N. 70th Street, Suite 100
Scottsdale, AZ 85266
1-888-896-7580
client-support@lazarusalliance.com
https://lazarusalliance.com